First Hit Previous Doc Next Doc Go to Doc#

Generate Collection Print

L13: Entry 21 of 28 File: EPAB Dec 2, 1999

PUB-NO: DE019823907A1
DOCUMENT-IDENTIFIER: DE 19823907 A1
TITLE: Issue and validation of ticket or permit cards

PUBN-DATE: December 2, 1999

INVENTOR-INFORMATION:

NAME	COUNTRY
HUETTINGER, STEPHAN	DE

ASSIGNEE-INFORMATION:

NAME	COUNTRY
FRAUNHOFER GES FORSCHUNG	DE

APPL-NO: DE19823907
APPL-DATE: May 28, 1998

PRIORITY-DATA: DE19823907A (May 28, 1998)

INT-CL (IPC): G07F 7/08; B42D 15/10; H04L 9/30
EUR-CL (EPC): B42D015/10 ; G07F007/10 , G07F017/42

ABSTRACT:

CHG DATE=20001128 STATUS=O>A ticket or permit is in the form of a card that has a coding that contains a digital signature that has a public section and a secret section. The issue of such cards or tickets takes place using two successive processing operations. The tickets or cards may be purchased over the internet and the user is allowed to print them on own printer.

Previous Doc Next Doc Go to Doc#

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 23 907 A 1**

(51) Int. Cl.[6]:
G 07 F 7/08
B 42 D 15/10
H 04 L 9/30
// B42D 109:00, 107:00

(21) Aktenzeichen: 198 23 907.6
(22) Anmeldetag: 28. 5. 98
(43) Offenlegungstag: 2. 12. 99

(71) Anmelder:
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., 80636 München, DE

(74) Vertreter:
Gagel, R., Dipl.-Phys.Univ. Dr.rer.nat., Pat.-Anw., 81241 München

(72) Erfinder:
Hüttinger, Stephan, Dipl.-Math., 64289 Darmstadt, DE

(56) Entgegenhaltungen:
DE 68 928 14 7T2
US 56 21 797
US 55 09 692
EP 07 13 198 A2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Bereitstellung von Berechtigungsnachweisen

(57) Die Erfindung betrifft ein Verfahren zur Bereitstellung von Berechtigungsnachweisen, insbesondere Eintrittskarten und Beförderungsscheinen, sowie die Ausgestaltung der bereitgestellten Berechtigungsnachweise.
Bei dem Verfahren werden an einer ersten Datenverarbeitungsstation Ausgangsdaten über den Gegenstand der Berechtigung erfaßt, eine erste Identifikationszeichenfolge für den Berechtigungsnachweis zugewiesen und die Daten auf Basis des geheimen Teils eines Signaturschlüssels digital signiert. Die digital signierten Daten werden dann über ein elektronisches Medium an eine zweite, von der ersten räumlich getrennte Datenverarbeitungsstation übermittelt, an der die signierten Daten auf ein maschinenlesbares Speichermedium übertragen werden, das als Berechtigungsnachweis dient.
Mit dem erfindungsgemäßen Verfahren lassen sich Eintritts- oder Fahrkarten online, d. h. beispielsweise über das Internet, verkaufen und bereitstellen. Das Verfahren ermöglicht einem Benutzer mit einem Computer mit Internetzugang und einem Drucker, seine Eintritts- oder Fahrkarte auf gewöhnlichem Papier selbst auszudrucken.

DE 198 23 907 A 1

DE 198 23 907 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren zur Bereitstellung von Berechtigungsnachweisen, insbesondere Eintrittskarten und Beförderungsscheinen, sowie die Ausgestaltung der bereitgestellten Berechtigungsnachweise. Sie stellt insbesondere ein System zur dezentralen, betrugssicheren Erstellung und Ausfertigung von Eintrittskarten, Fahrkarten, Flugtikkets und anderen Tickets über elektronische Netze zur Verfügung.

Das Anwendungsgebiet des erfindungsgemäßen Verfahrens fällt in den Bereich des elektronischen Handels über Computernetzwerke, wie das Internet. Eingebunden in Strukturen des elektronischen Handels, wie sogenannte Online-Bezahlprotokolle und kryptographisch gesicherte Internetkommunikation, ermöglicht die Erfindung den Online-Verkauf und den Online-Vertrieb von Eintritts- und Fahrkarten, sowie deren automatisierbare Kontrolle.

Die gängigen Verfahren zur Bereitstellung von Berechtigungsnachweisen wie Eintrittskarten oder Fahrkarten werden im folgenden kurz diskutiert.

Der Erwerb von Eintrittskarten für kulturelle Veranstaltungen kann über eine telefonische Vorbestellung, über den direkten Erwerb in einer Vorverkaufsstelle, über den direkten Erwerb an der Abendkasse oder über eine Bestellung über das Internet erfolgen.

Bei einer Vorbestellung der Eintrittskarte muß diese jedoch üblicherweise eine halbe Stunde vor Beginn der Vorstellung abgeholt werden. Für das Abholen selbst muß sich der Kunde in der Regel noch einmal in eine Reihe einreihen.

Beim Erwerb in einer Vorverkaufsstelle sind zusätzliche Wege zu den selten dezentral bestehenden Vorverkaufsstellen notwendig.

Der Erwerb der Eintrittskarten an der Abendkasse birgt das Risiko, daß keine Eintrittskarten mehr verfügbar sind. In der Regel muß sich der Kunde auch hier zunächst in eine Schlange einreihen.

Beim Kauf der Eintrittskarte über das Internet wird diese zugeschickt oder muß am Ort der Veranstaltung abgeholt werden. Das Zuschicken dauert in der Regel mindestens einen Werktag. Für den spontan oder kurzfristig geplanten Besuch einer Veranstaltung ist diese Methode daher nicht geeignet. Wenn die Eintrittskarte vor Ort abgeholt werden soll, muß sich der Kunde dafür wieder unnötig anstellen. Bei gut besuchten Veranstaltungen dauert das in der Regel länger als nur ein paar Minuten.

Eine Bahnfahrkarte kann beispielsweise direkt an einem Schalter der Bundesbahn oder über das Internet erworben werden.

Der Kauf am Bahnschalter ist jedoch im allgemeinen zeitraubend und nervenaufreibend. Es besteht sogar die Gefahr, durch die Wartezeit den Zug zu verpassen.

Beim Kauf der Fahrkarte über das Internet erfolgt die Zusendung der Fahrkarte über den Postweg. Dies dauert mindestens einen Werktag. Diese Methode läßt daher eine kurzfristige Reiseplanung nicht zu.

Der Kauf einer Bahnfahrkarte oder eines Flugtickets in einem Reisebüro hat den Nachteil, daß hierfür extra ein Reisebüro aufgesucht werden muß. Läßt sich der Kunde die Fahrkarte oder das Ticket zuschicken, so erfordert dies eine längerfristige Reiseplanung.

Alle bekannten Methoden zum Erwerb einer Eintrittskarte oder Fahrkarte, zeichnen sich daher durch zum Teil umständliche und zeitraubende Prozeduren der Bereitstellung dieser Berechtigungsnachweise aus.

Es ist daher eine Aufgabe der vorliegenden Erfindung, ein Verfahren zur Bereitstellung von Berechtigungsnachweisen, insbesondere Eintrittskarten und Beförderungsscheinen, sowie eine Ausgestaltung eines Berechtigungsnachweises anzugeben, mit denen die obigen Nachteile für Kunden, im folgenden Benutzer genannt, vermieden werden können und die eine sichere und schnelle Bereitstellung des Berechtigungsnachweises ermöglichen.

Die Aufgabe wird mit dem Verfahren nach Anspruch 1 bzw. dem Berechtigungsnachweis nach Anspruch 13 gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind Gegenstand der Unteransprüche.

Beim erfindungsgemäßen Verfahren werden an einer ersten, vorzugsweise zentralen Datenverarbeitungsstation, beispielsweise einem Ticketserver, Ausgangsdaten über den Gegenstand der Berechtigung erfaßt. Diese Ausgangsdaten oder die Information über eine Auswahl aus einer Vielzahl von an der Datenverarbeitungsstation bereits vorliegenden Ausgangsdaten können der ersten Datenverarbeitungsstation von einer zweiten Datenverarbeitungsstation, beispielsweise dem privaten Computer eines Benutzers, über ein elektronisches Medium wie das Internet zugeführt werden. An der ersten Datenverarbeitungsstation wird dem zu erstellenden Berechtigungsnachweis eine erste, eindeutige Identifikationszeichenfolge (im folgenden als Ticket-ID bezeichnet) zugewiesen. Desweiteren wird ein Signaturschlüssel mit einem öffentlichen Teil und einem geheimen Teil zur Verfügung gestellt. Schließlich werden signierte Daten durch digitales Signieren zumindest der Ausgangsdaten und der ersten Identifikationszeichenfolge auf Basis des geheimen Teils des Signaturschlüssels erzeugt. Die signierten Daten werden über ein elektronisches Medium an die zweite, von der ersten räumlich getrennte Datenverarbeitungsstation, beispielsweise den Computer des Benutzers, übermittelt. An der zweiten Datenverarbeitungsstation werden die signierten Daten auf ein maschinenlesbares Speichermedium übertragen, das als Berechtigungsnachweis dient.

Bei dem Signaturschlüssel, der an der ersten Datenverarbeitungsstation zur Verfügung gestellt wird, handelt es sich beispielsweise um den Signaturschlüssel eines Veranstalters. Dieser Signaturschlüssel wird für alle Berechtigungsnachweise desselben Veranstalters oder derselben Veranstaltung eingesetzt und ist daher unabhängig von dem einzelnen Berechtigungsnachweis. Aus Sicherheitsgründen wird der Signaturschlüssel in der Regel einmal jährlich gewechselt.

In einer bevorzugten Ausführungsform wird an der ersten Datenverarbeitungsstation eine weitere Identifikationszeichenfolge für ein Berechtigungsmedium (im folgenden als Ticket-Card bezeichnet) erfaßt, wobei diese weitere Identifikationszeichenfolge ebenfalls, zusammen mit den anderen Daten, digital signiert wird. Das Berechtigungsmedium mit der Identifikationszeichenfolge wird dem Benutzer unabhängig von der Bereitstellung des Berechtigungsnachweises zur Verfügung gestellt und ist nicht auf die Verwendung mit dem gerade auszustellenden Berechtigungsnachweis beschränkt.

Mit dem erfindungsgemäßen Verfahren lassen sich Eintritts- oder Fahrkarten online, d. h. beispielsweise über das Internet, verkaufen und bereitstellen. Das Verfahren kann die aufkommenden Strukturen des elektronischen Handels, wie Online-Bezahlprotokolle, oder die des Mechanismus der digitalen Signatur nutzen (vgl. z. B. A. Beutelsbacher et al., "Moderne Verfahren der Kryptographie", Vieweg, 1995, ISBN 3-528-06590-7 oder A. J. Menezes et al., "Handbook of Applied Cryptography", CRC Press, 1997, ISBN 0-8493-8523-7). Der Aufbau dieser Strukturen wird insbesondere durch das 1997 in Kraft getretene Signaturgesetz (SiG vom 22.07.1997, BGBl I S. 1870, 1872) gefördert und beschleunigt.

In einer bevorzugten Ausführungsform der Erfindung erfolgt das Übermitteln der signierten Daten in Form einer

Graphikdatei, die die signierten Daten in graphischer Darstellung, beispielsweise als 2D Bar Code Repräsentation und in ASCII-Darstellung, enthält. Die übermittelte Graphikdatei kann dann auf einem bedruckbaren Träger, insbesondere Papier, ausgedruckt werden.

Dies ermöglicht dem Benutzer, seine Eintrittskarte oder Fahrkarte selbst zu erstellen. Sofern der Benutzer über einen Internetanschluß und einen handelsüblichen Drucker verfügt, kann er sich die Eintritts- oder Fahrkarte auf gewöhnlichem Papier ausdrucken.

Das Verfahren schließt in Verbindung mit weiter unten beschriebenen Kontrollmaßnahmen aus, daß der Benutzer ohne Mitwirkung des Veranstalters Eintritts- oder Fahrkarten erstellen kann, und es schließt aus, daß der Benutzer oder Dritte illegal erzeugte Kopien der ausgedruckten Karten verwenden können.

Alle oben dargestellten Nachteile des Standes der Technik können beim Einsatz des erfindungsgemäßen Verfahrens vermieden werden. Das bedeutet, daß kein Anstellen, Vorbestellen, Aufsuchen von Reisebüros oder Vorverkaufsstellen nötig ist, um eine Eintritts- oder Fahrkarte zu erwerben. Dies gilt unter der Voraussetzung, daß der Benutzer über einen Internetanschluß und einen Drucker verfügt. Weiterhin müssen die Modalitäten für die Bezahlung der Karte geklärt sein, beispielsweise durch Schaffen der Voraussetzungen für wenigstens ein Online-Bezahlprotokoll (vgl. z. B. O'Mahony et al., "Electronic Payment Systems", Artech House Publishers, 1997, ISBN 0-89006-925-5) auf Benutzer- wie auf Veranstalterseite. Der Veranstalter muß für die Kontrolle der Eintritts-/Fahrkarte über einen Computer und über ein Lesegerät verfügen. Wird die 2D Bar Code Technik zur maschinenlesbaren Repräsentation der Daten auf der Eintritts-/Fahrkarte verwendet, eignet sich für das Lesegerät ein CCD Scanner.

Die Erfindung ermöglicht in vorteilhafter Weise die Bereitstellung bzw. den Verkauf und Vertrieb von Eintrittskarten (Kino, Theater, Konzert, ...) oder Fahrkarten (z. B. Bundesbahn, Flugticket) über das Internet. Auf einem sogenannten Ticketserver des Veranstalters werden die Eintritts-/Fahrkarten erzeugt. Über das Internet wird die Eintritts-/Fahrkarte an den Käufer übermittelt. Der Käufer druckt die Eintritts-/Fahrkarte auf seinem eigenen Drucker auf gewöhnlichem Papier aus.

Die Eintritts-/Fahrkarte kann nur vom Veranstalter erzeugt werden. Vom Käufer illegal erzeugte Kopien der Eintritts-/Fahrkarte können nicht verwendet werden.

Die Kontrolle der Eintritts-/Fahrkarte auf Veranstalterseite ist voll automatisierbar. Erworbene und nicht benutzte Eintritts-/Fahrkarten können erkannt werden.

Im folgenden wird das erfindungsgemäße Verfahren anhand dreier beispielhafter Ausführungsformen näher erläutert. Zur Vereinfachung wird hierbei der Begriff "Veranstaltung" sowohl für eine kulturelle Veranstaltung als auch für eine Bahnfahrt oder einen Flug verwendet. Der Ausdruck "Eintrittskarte" wird synonym für Eintrittskarte und Fahrkarte verwendet.

Gemäß einer ersten, weitergebildeten Ausführungsform des erfindungsgemäßen Verfahrens besteht die für eine Veranstaltung gültige Zugangsberechtigung aus zwei Teilen. Der eine Teil betrifft ein Berechtigungsmedium, im folgenden TicketCard genannt, der andere Teil die Eintrittskarte selbst, im folgenden Ticket genannt. Die TicketCard ist nur Träger einer eindeutigen Nummer, im folgenden TicketCard ID genannt.

Die TicketCard wird vom Benutzer einmalig offline erworben, beispielsweise an einer Kino- oder Theater-Kasse, an einem Fahrkartenschalter, in einer Reisebüro oder Post, oder auf sonstige Weise. Sie ist wieder verwendbar. Die TicketCard entspricht in Ausführungs- und Fertigungsqualität einer Kreditkarte oder einer Bundesbahn BahnCard und verfügt daher über dasselbe hohe Maß an Fälschungssicherheit. Auf der TicketCard sind nur eine eindeutige Identifikationsnummer, die TicketCard ID, und der Gültigkeitszeitraum der Karte gespeichert, beides in ASCII Repräsentation und in maschinenlesbarer Form. Für die maschinenlesbare Form bietet sich die Repräsentation als Bar Code an (vgl. z. B. R. Palmer, "The Bar Code Book", Helmers Publishers, 1995, ISBN 0-911261-09-5). Sie kann aber auch in anderer Form über einen Magnetstreifen oder einen Speicherchip erfolgen. Die TicketCard beinhaltet keine Informationen über den Inhaber der Karte oder über die Veranstaltung für die sie eingesetzt wird. Sie ist somit übertragbar und für jede Veranstaltung einsetzbar, die das Verfahren unterstützt. Die TicketCard dient nur als Verbindungsglied zu dem Ticket, dem zweiten Bestandteil der Zugangsberechtigung. Sie dient nicht zum Anlegen eines Benutzerprofils. Die TicketCard hat keine Bezahlfunktion.

Das Ticket beinhaltet alle im Rahmen der Veranstaltung relevanten Informationen (z. B. Ort, Datum, Sitznummer, Preiskategorie, Fahrtstrecke, ...), sowie im vorliegenden Beispiel drei Identifikationsnummern. Dies sind dieselbe TicketCard ID wie sie auf der TicketCard des Benutzers steht, eine zur eindeutigen Identifizierung des Tickets verwendbare Nummer, die sogenannte Ticket ID, und die sogenannte Key ID, die zur eindeutigen Identifizierung des öffentlichen Teils des verwendeten Signaturschlüssels dient. Die Veranstaltungsparameter werden vom Benutzer online ausgewählt. Die TicketCard ID erhält er von seiner TicketCard, und die Ticket ID sowie die Key ID gibt der Veranstalter vor. Nachdem der Benutzer online die Veranstaltungsparameter ausgewählt und seine TicketCard ID angegeben hat, werden diese Daten an den Ticketserver des Veranstalters übertragen. Zu den erhaltenen Daten, der Ticket ID und der Key ID erzeugt der Ticketserver dann eine digitale Signatur mit dem geheimen Part seines Signaturschlüssels. Eine ASCII, sowie eine 2D Bar Code (zweidimensionaler Bar Code) Repräsentation der signierten Daten werden vom Ticketserver in eine Graphikdatei umgewandelt.

Vor oder nach Erstellung des Tickets durch den Ticketserver sollten Benutzer und Ticketserver ein Bezahlprotokoll ausgehandelt haben, und es sollten entsprechende Daten vom Benutzer übertragen und vom Ticketserver überprüft worden sein. Wenn das Bezahlprotokoll positiv abgewickelt worden ist, sendet der Ticketserver die Graphikdatei an den Web Browser des Benutzers, beispielsweise als HTTP Response. Der Benutzer druckt die Graphikdatei aus und erhält so sein Ticket.

In dem beschriebenen Ablauf signiert der Ticketserver u. a. die vom Benutzer angegebene TicketCard ID. Dem Ticketserver ist zwar nicht der Benutzer bekannt, aber seine TicketCard ID. Diese kann er zur Erstellung eines Nutzungsprofiles der Ticketcard benutzen.

Im folgenden wird in einer zweiten, weitergebildeten Ausführungsform der Erfindung ein alternatives Verfahren vorgestellt, bei dem der Ticketserver die TicketCard ID des Benutzers nicht erkennt, und er sie somit nicht zur Erstellung eines Nutzungsprofiles verwenden kann.

Gemäß dieser zweiten Ausführungsform besteht wie bei der ersten Ausführungsform die für eine Veranstaltung erforderliche Zugangsberechtigung aus einer Ticketcard und einem Ticket. Die vom Benutzer ausgewählten Parameter, die Ticket ID und die Key ID werden vom Ticketserver digital signiert. Die Ticketcard ID hingegen wird vom Ticketserver mittels der Technik der blinden Signatur signiert. Bei der blinden Signatur erkennt der Unterzeichner weder was er unterzeichnet, noch die eigentliche [illegible]. Bei-

spiele für die Erzeugung einer blinden Signatur sind beispielsweise aus A. Beutelsbacher et al., "Moderne Verfahren der Kryptographie", Vieweg, 1995, ISBN 3-528-06590-7 oder aus A. J. Menezes et al., "Handbook of Applied Cryptography", CRC Press, 1997, ISBN 0-8493-8523-7 zu entnehmen.

Durch die blinde Signatur erhält der Ticketserver keine Kenntnis von der TicketCard ID, und kann diese somit nicht als einen Schlüssel für ein Nutzungsprofil verwenden. Die TicketCard ID soll aber in lesbarer Form Bestandteil des Tickets sein. Da die ID dem Ticketserver nur in "blinder" Form vorliegt, kann somit die das Ticket enthaltende Graphikdatei nicht vom Ticketserver erstellt werden. Statt dessen erfolgt die Umwandlung der signierten Daten, sowohl in ASCII als auch in 2D Bar Code Repräsentation, in die Graphikdatei auf Benutzerseite, beispielsweise durch ein entsprechendes Applet. Dies ist möglich, da auf Benutzerseite die blinde Signatur der TicketCard ID wieder in eine konventionelle digitale Signatur umgewandelt werden kann.

Alternativ zur blinden Signatur kann auch durch Verwendung einer Hashfunktion und einer vom Rechner des Benutzers erzeugten Zufallszahl sichergestellt werden, daß der Ticketserver bei der Signatur keine Kenntnis von der TicketCard ID des Benutzers erhält. Dafür bildet der Rechner des Benutzers den Hashwert über die TicketCard ID und eine Zufallszahl und sendet diesen an den Ticketserver. Der Hashwert, die Ticket ID, die Key ID sowie die vom Benutzer ausgewählten Parameter werden vom Ticketserver digital signiert und an den Benutzer zurückgesandt.

Auf Benutzerseite werden die signierten Daten und die Zufallszahl in maschinenlesbarer Form und in ASCII Form in eine Graphikdatei integriert. Durch die geschilderte Verwendung der Hashfunktion ist die Bindung von TicketCard ID und Ticket garantiert. Durch Verwendung der Zufallszahl drückt sich diese Bindung durch einen pro Veranstaltung einmaligen Hashwert aus, so daß der Hashwert nicht als Schlüssel für ein Nutzungsprofil geeignet ist.

Die eigentliche Zugangsberechtigung zu der Veranstaltung besteht bei beiden Ausführungsformen aus der Kombination von TicketCard und Ticket.

In der nachfolgend dargestellten dritten Ausführungsform der Erfindung besteht die Zugangsberechtigung nur aus dem Ticket, wie es in der ersten Ausführungsform der Erfindung beschrieben worden ist.

Bei dieser dritten Ausführungsform des Verfahrens ist die TicketCard nicht zwingend erforderlich. Die für eine Veranstaltung gültige Eintrittskarte besteht nur aus dem Ticket. Die vom Benutzer ausgewählten Parameter, die Ticket ID und die Key ID werden vom Ticketserver digital signiert. Eine ASCII, sowie eine 2D Bar Code Repräsentation der signierten Daten werden vom Ticketserver in eine Graphikdatei umgewandelt. Nach Erstellung des Tickets und erfolgreicher Abwicklung eines Bezahlprotokolls sendet der Ticketserver die Graphikdatei an den Web Browser des Benutzers, beispielsweise als HTTP-Response. Der Benutzer druckt die Graphikdatei aus und erhält so sein Ticket.

Die TicketCard gemäß der ersten und zweiten Ausführungsform ist für alle Veranstaltungen dieselbe. Durch Verwendung der TicketCard ist es auf Veranstalterseite nicht notwendig die IDs bereits erfolgreich kontrollierter Tickets zu speichern. Ohne eine TicketCard in der dritten Ausführungsform ist dies notwendig, um zu verhindern, daß vom Benutzer illegal erzeugte Kopien eines Tickets als gültige Eintrittskarten betrachtet werden.

Das Ticket wird in allen drei Ausführungsformen des Verfahrens für jede Veranstaltung neu vom Veranstalter erzeugt und vom Benutzer auf einem eigenen Drucker ausgedruckt. Die Repräsentation auf dem vom Benutzer erstellten Ticket erfolgt in ASCII und in maschinenlesbarer Form. Die ASCII Repräsentation garantiert, daß die Daten auch ohne technische Hilfsmittel gelesen werden können. Die Repräsentation in einer maschinenlesbaren Form ist für eine zuverlässige und schnelle Kontrolle notwendig. Wesentlicher Bestandteil der Kontrolle ist die Überprüfung der digitalen Signatur der Ticketdaten. Dies kann nur maschinell geschehen und nicht durch Augenschein.

Die Wahl der 2D Bar Code Technik als zur Zeit geeignetste maschinenlesbare Repräsentation der Ticketdaten ergibt sich aus folgenden Anforderungen an das Ticket.

Die Daten müssen an der Kontrollstation schnell gelesen werden können. Aufgrund dieser Anforderung ist beispielsweise eine Diskette als Trägermedium nicht von Vorteil.

Die maschinenlesbare Repräsentation der Ticketdaten muß vom Benutzer mit möglichst wenig Aufwand erstellt werden können. Über ein Magnetstreifenschreibgerät oder ein Speicherchipschreibgerät verfügen zur Zeit und wohl auch in naher Zukunft die wenigsten Benutzer. Deshalb scheiden zur Zeit Magnetstreifenkarten oder Chipkarten in den bevorzugten Ausführungsformen als Träger der Ticketdaten aus. Über einen Drucker hingegen verfügt fast jeder Benutzer.

Magnetstreifenkarten oder Chipkarten können jedoch dann eingesetzt werden, wenn die Tickets nicht vom Benutzer selbst, sondern an entsprechend dafür vorgesehenen dezentralen Verkaufsstellen erstellt werden. Hierbei muß der Benutzer allerdings wieder entsprechende Nachteile durch das Abholen der Tickets in Kauf nehmen.

Aus den Anforderungen ergibt sich, daß das zur Zeit geeignetste Trägermedium für die maschinenlesbare Repräsentation der Ticketdaten Papier ist. Eine geeignete maschinenlesbare Repräsentationsform von Daten auf Papier stellt die Bar Code Technik dar, insbesondere die 2D Bar Code Technik zur Speicherung großer Datenmengen. Generell gilt jedoch, daß die vorgestellten drei Ausführungsformen des Verfahrens unabhängig von der Repräsentationsform der Daten sind.

Kein Bestandteil der Erfindung ist die Sicherung der Kommunikation zwischen dem Web Browser des Benutzers und dem Server des Veranstalters. Hierzu sind bereits eine Vielzahl von Mechanismen bekannt und realisiert. Ebenfalls sind Bezahlprotokolle, sowie Sicherheitsaspekte im Zusammenhang mit möglichen Bezahlprotokollen kein Bestandteil der Erfindung.

Die Erfindung bietet jedoch in allen drei Ausführungsformen eine Lösung für folgende Sicherheitsanforderungen:
Das Ticket und damit die Eintrittskarte soll nur vom Veranstalter erzeugt werden können.

Vom Käufer illegal erzeugte Kopien der Eintrittskarte sollen nicht verwendet werden können.

Die TicketCard entspricht in Ausführungs- und Fertigungsqualität einer Kreditkarte oder einer Bundesbahn BahnCard und erfüllt daher denselben hohen Sicherheitsstandard hinsichtlich Fälschungs- und Manipulationssicherheit (beispielsweise durch das integrierte Hologramm). Somit kann die TicketCard nicht ohne erheblichen Aufwand nachgemacht oder ohne sichtbare Schädigung manipuliert werden.

Die verwendete Technik der digitalen Signatur garantiert, daß gültige Tickets nur vom Veranstalter erzeugt werden können, bzw. daß Tickets, die nicht vom Veranstalter erzeugt worden sind, als solche erkannt werden können. Die Kopplung des leicht kopierbaren Tickets an die nicht kopierbare Ticketcard bewirkt, daß die Eintrittskarte als Kombination von Ticket und TicketCard nicht kopiert werden kann. Außerdem kann die Eintrittskarte nur vom Veranstalter erzeugt werden.

Bei der dritten Ausführungsform des Verfahrens beruht der Schutz vor dem Mißbrauch von Kopien eines Tickets auf der Speicherung bereits erfolgreich kontrollierter Tikkets. Jede Kontrollstation muß also auf alle im Rahmen der Veranstaltung bereits erfolgreich kontrollierten Tickets zugreifen können. Diese Notwendigkeit entfällt bei Verwendung der TicketCard gemäß der ersten und zweiten Ausführungsform des Verfahrens.

Für die Kontrolle auf Veranstalterseite werden zwei mögliche Kontrollverfahren der Eintrittskarte vorgestellt. Es besteht keine Korrelation zwischen "Kontrollverfahren A" und "Kontrollverfahren B" und den als erste und zweite Ausführungsform des Verfahrens vorgestellten Möglichkeiten der Bereitstellung der Eintrittskarte.

Das Kontrollverfahren A ist geeignet für die gemäß der ersten und zweiten Ausführungsform bereitgestellten Tikkets. Es ist nicht für die gemäß der dritten Ausführungsform bereitgestellten Tickets geeignet, da hier der Benutzer über keine TicketCard verfügt.

Die Zugangsberechtigung des Benutzers besteht aus seiner TicketCard und dem Ticket. Zur Kontrolle der Eintrittskarte zeigt der Benutzer seine TicketCard und sein Ticket vor. Über einen Bar Code Leser werden von der TicketCard die TicketCard ID und die Gültigkeitsdauer und von dem Ticket die digital signierten Daten eingelesen. Ist für die TicketCard und/oder das Ticket eine andere maschinenlesbare Repräsentationsform gewählt worden, sind selbstverständlich entsprechend andere Lesegeräte zu verwenden. Die digital signierten Daten beinhalten, die Veranstaltungsparameter (Ort, Zeit, Preiskategorie, Platz, Fahrtstrecke, ...), eine TicketCard ID, eine Ticket ID und eine Key ID. Folgendes wird automatisch überprüft:

1. Ist die TicketCard noch gültig.
2. Sind die TicketCard IDs, die von der TicketCard gelesene und die vom Ticket gelesene, identisch.
3. Stimmen die Veranstaltungsparameter mit der aktuellen Veranstaltung überein.
4. Ist die digitale Signatur des Tickets gültig.

Um Punkt 4. entscheiden zu können, benötigt der Rechner der Kontrollstation den öffentlichen Part des Signaturschlüssels des Veranstalters. Dieser ist eindeutig durch die Key ID identifizierbar. Abgesehen von dem Schlüssel befinden sich alle für die Kontrolle von 1. bis 4. notwendigen Daten auf der TicketCard und auf dem Ticket. Es ist auch möglich, den öffentlichen Part des verwendeten Signaturschlüssels direkt auf dem Ticket zu speichern. In der Regel ist das Lesen des Schlüssels vom Ticket jedoch langsamer als das Lesen des Schlüssels aus dem Speicher des Kontrollrechners, so daß letzteres vorgezogen wird.

Wenn die Veranstaltung durch die Veranstaltungsparameter auf dem Ticket eindeutig bestimmt ist, dann ist die Eintrittskarte des Benutzers genau dann gültig, wenn alle vier Überprüfungen positiv ausfallen.

In besonders gelagerten Fällen kann auch eine andere Lösung erforderlich sein, wie das folgende Beispiel zeigt. Eine Bundesbahnfahrkarte über 100 km ist für vier Tage gültig. Ein Ticket, das Teil einer vier Tage gültigen Fahrkarte ist, bestimmt nicht eindeutig die einmalige Fahrt für die es verwendet ist. Denn wenn bei einer Kontrolle der Fahrschein nicht bestimmt werden kann, ob diese schon einmal kontrolliert worden ist, dann kann die Fahrkarte in diesen Fällen beliebig oft verwendet werden, obwohl sie nur für eine einmalige Fahrt ausgestellt worden ist. Für dieses Problem gibt es verschiedene Lösungsansätze.

Das Ticket verfügt neben der TicketCard ID über eine Ticket ID. Diese kann als Schlüssel für einen Datensatz dienen, der nach der ersten Kontrolle erzeugt wird. Der Datensatz ist so zu speichern, daß bei jeder Kontrolle während der Gültigkeit des Tickets auf ihn zugegriffen werden kann. Dadurch können während der gesamten Fahrt die Tickets identifiziert werden, die schon einmal für die Strecke verwendet worden sind. Denkbar ist etwa, daß die Kontrolleinheit jedes Schaffners über Funk eine Verbindung zu einem Rechner im Zug unterhält. Der Rechner selbst unterhält eine Funkverbindung zu einem stationären Zentralrechner, der für die Verwaltung der kontrollierten Tickets auf der entsprechenden Strecke zuständig ist. Durch den Einsatz des Zugrechners ist nur eine geringe Reichweite der mobilen Kontrollstationen erforderlich.

Eine andere Möglichkeit besteht darin, online nur Tickets mit beschränkter Gültigkeit zu erstellen. Die Beschränkung ist so zu wählen, daß das geschilderte Problem der unerlaubten Mehrfachnutzung nicht auftreten kann. Sinnvollerweise ist deshalb die Länge der Gültigkeitsdauer in Abhängigkeit von der erwarteten Fahrtdauer zu wählen. Falls der Benutzer das Ticket in diesem Zeitraum nicht nutzen konnte, kann er online eine Rückerstattung des Fahrpreises beantragen und ein neues Ticket erwerben. Der Ticketserver kann entscheiden, ob die Rückerstattung des Fahrpreises gerechtfertigt ist, d. h. ob das entsprechende Ticket tatsächlich nicht benutzt worden ist, wenn die IDs aller im entsprechenden Gültigkeitszeitraums kontrollierten Tickets dem Ticketserver vorliegen. Diese Daten erhält der Ticketserver von den einzelnen Kontrollstationen. Dies kann automatisch geschehen, indem beispielsweise jeder Schaffner am Ende seines Arbeitstages sein Kontrollgerät an einen Rechner andockt und dieser Rechner die Daten an den Ticketserver übermittelt. Als Schlüssel für die Datensätze werden die Ticket IDs verwendet.

Das andere Kontrollverfahren, Kontrollverfahren B, ist für alle drei vorgestellten Ausführungsformen des erfindungsgemäßen Verfahrens der Bereitstellung der Tickets geeignet. Die TicketCard ist hierfür nicht erforderlich. Dieses Kontrollverfahren ist nur für Veranstaltungen geeignet, in denen der Benutzer garantiert zu Beginn kontrolliert wird, so daß der Benutzer später eine erfolgte erfolgreiche Kontrolle nachweisen kann, indem er z. B. ein vom Veranstalter markiertes Ticket vorzeigt. Eine Eintrittskartenkontrolle erfolgt beispielsweise garantiert zu Beginn der Veranstaltung im Kino, im Theater, bei Konzerten oder bei Sportveranstaltungen.

Die Eintrittskarte des Benützers besteht nur aus seinem Ticket. Zur Kontrolle der Eintrittskarte zeigt der Benutzer sein Ticket vor. Über einen Bar Code Leser werden von dem Ticket die digital signierten Daten eingelesen. Die digital signierten Daten beinhalten, die Veranstaltungsparameter (Ort, Zeit, Preiskategorie, Platz, Fahrstrecke, ...), möglicherweise eine TicketCard ID (wird nicht weiter verwendet), eine Ticket ID und eine Key ID. Folgendes wird bei einer ersten Kontrolle automatisch überprüft:

1. Stimmen die Veranstaltungsparameter mit der aktuellen Veranstaltung überein.
2. Ist die digitale Signatur des Tickets gültig.
3. Ist dies das erste Mal, das ein Ticket mit der gegebenen Ticket ID überprüft wird, für welches 1. und 2. erfolgreich überprüft worden sind.

Um Punkt 3. entscheiden zu können, benötigt der Rechner der Kontrollstation den öffentlichen Part des Signaturschlüssels des Veranstalters. Dieser ist eindeutig durch die Key ID identifizierbar. Um 3. entscheiden zu können muß die Kontrollstation auf eine Datenbank haben, in der alle bereits [illegible] überprüften Tickets gespeichert sind.

Das Ticket ist nur dann gültig, wenn alle drei Überprüfungen positiv ausfallen. Ist dies der Fall, wird das Ticket vom Veranstalter als gültig markiert. Ein nicht als gültig markiertes Ticket, das eine der drei Überprüfungen nicht besteht, wird als ungültig angesehen.

Falls der Veranstalter die Erstattung nicht verwendeter Eintrittskarten unterstützt, muß nach erfolgreicher Überprüfung die Ticket ID gespeichert werden. Eine Eintrittskarte kann als nicht verwendet identifiziert werden, wenn das zugehörige Ticket erstellt worden ist und die Ticket ID nicht in der Datenbank der erfolgreich überprüften Eintrittskarten gespeichert ist. Der Antrag auf Erstattung einer nicht benutzten Eintrittskarte kann online gestellt und bearbeitet werden.

Im Rahmen der Ticketerstellung erhält der Ticketserver keine personenbezogenen Daten, wie beispielsweise den Benutzernamen. Die einzige Information, die sich als Schlüssel für ein Benutzerprofil eignet ist die TicketCard ID. Der Ticketserver kann über die TicketCard ID erstellte Tickets einer Ticketcard zuordnen. Der Schluß, daß die entsprechenden Veranstaltungen von derselben Person besucht worden sind, ist aber nicht zulässig, da die TicketCard übertragbar ist. Daher kann über die TicketCard ID lediglich ein Nutzungsprofil der TicketCard erstellt werden.

Wie anhand der zweiten Ausführungsform gezeigt wurde, läßt sich aber auch dies verhindern. Durch Einsatz der Technik der blinden Signatur wird verhindert, daß der Ticketserver beim Signieren Kenntnis von der TicketCard ID erhält. In diesem Fall besteht daher für den Ticketserver keine Möglichkeit, ein Nutzungsprofil der Ticketcard anzulegen.

Sehr wohl geeignet zur Erstellung eines Benutzer- oder Nutzungsprofils, sind jedoch möglicherweise Daten, die im Rahmen eines Bezahlprotokolls an den Ticketserver übermittelt werden. Dies kann nur durch Wahl eines geeigneten Bezahlprotokolls vermieden werden und liegt nicht im Rahmen der vorgestellten Erfindung.

Im folgenden wird die Erfindung nochmals anhand eines konkreten Ausführungsbeispiels in Verbindung mit den Figuren erläutert. Hierbei zeigen

Fig. 1 ein Beispiel für ein Berechtigungsmedium in Form einer TicketCard für kulturelle Veranstaltungen, im folgenden auch CulturCard genannt, zur Verwendung in Kombination mit einem erfindungsgemäß bereitgestellten Berechtigungsnachweis bzw. Ticket;

Fig. 2 ein Beispiel für digital signierte Veranstaltungsparameter und IDs gemäß der vorliegenden Erfindung;

Fig. 3 eine 2D Bar Code Repräsentation der signierten Daten aus **Fig.** 2; und

Fig. 4 ein auf Grundlage der Daten der **Fig.** 2 gemäß der vorliegenden Erfindung vom Benutzer ausgedrucktes Ticket, das dem Benutzer als Graphikdatei übermittelt wurde

In diesem Ausführungsbeispiel wird eine Eintrittskarte nach der ersten Ausführungsform des Verfahrens erstellt Die Kontrolle des erstellten Tickets erfolgt nach Kontrollverfahren A.

In Zusammenhang mit kulturellen Veranstaltungen, beispielsweise Kino, Theater oder Konzert, wird die TicketCard aus Gründen der Eingängigkeit im folgenden als CulturCard bezeichnet. Für den Zugang zu der Veranstaltung benötigt der Benutzer bei diesem Beispiel eine CulturCard in Verbindung mit einem Ticket. Die CulturCard wird einmalig offline erworben, das Ticket pro Veranstaltung online

Der Benutzer erwirbt offline eine CulturCard. Ein Beispiel einer CulturCard ist in **Fig.** 1 dargestellt. Wie aus der Figur zu erkennen ist, sind auf der CulturCard nur die Gültigkeitsdauer und eine eindeutige Identifikationsnummer ("7492 1068"), CulturCard ID genannt, gespeichert, beide in ASCII Repräsentation und in maschinenlesbarer Form Bar Code.

Es sind also insbesondere keine personenbezogenen Daten auf der CulturCard vorhanden. Die CulturCard ist nicht an einen bestimmten Benutzer gebunden. In Größe und Fertigungsqualität entspricht die CulturCard einer gängigen Kreditkarte oder Bundesbahn BahnCard.

Der Benutzer verfügt über ein Computerterminal, welches an das Internet angeschlossen ist, sowie über einen Drucker. Das erfindungsgemäße Verfahren umfaßt im vorliegenden Beispiel folgende Schritte:

1. Der Benutzer ruft über den Web Browser die Web-Seite des Veranstalters auf und stellt so eine Online-Verbindung zum Ticketserver des Veranstalters her.
2. Der Benutzer wählt eine Veranstaltung aus. Daraufhin zeigt der Ticketserver dem Benutzer die Parameter an, die für die Wahl des Tickets von Bedeutung sind. Dies können Ort und Zeitpunkt der Veranstaltung, Preiskategorie, noch freie Plätze, usw. umfassen. Im Theaterkontext ist denkbar, daß der Ticketserver online eine realistische Bühnensicht anbietet. Klickt der Benutzer etwa auf einen freien Platz in der schematischen Sitzplatzverteilung, zeigt der Ticketserver einen relevanten Bühnenausschnitt, wie er von diesem Platz aus wahrgenommen werden würde.
3. Der Benutzer wählt die Parameter aus und entscheidet sich für eines der vom Ticketserver unterstützen Bezahlprotokolle. Außerdem gibt er die ID seiner CulturCard ein (hier: "7492 1068").
4. Nach erfolgreichem Abschluß der Aktionen, die mit dem Bezahlprotokoll verbunden sind, erstellt der Tikketserver das Ticket. Dazu werden die vom Benutzer ausgewählten Parameter, die CulturCard ID, die vom Server erzeugte Ticket ID und die Key ID vom Ticketserver digital signiert, wie dies in **Fig.** 2 beispielhaft dargestellt ist.
5. Der Server erstellt eine Graphikdatei, welche eine ASCII-Repräsentation der Veranstaltungsparameter und der IDs sowie eine 2D Bar Code Repräsentation derselben Information als digital signierte Daten enthält. **Fig.** 3 zeigt die 2D Bar Code Repräsentation der digital signierten Daten. Die Graphikdatei wird an den Web Browser des Benutzers übermittelt, beispielsweise als HTTP Response.
6. Der Benutzer druckt die Graphikdatei aus und schneidet das Ticket aus, das in **Fig.** 4 dargestellt ist. Die Zugangsberechtigung für die Veranstaltung setzt sich aus der CulturCard (**Fig.** 1) und dem Ticket (**Fig.** 4) zusammen.

Bei der Kontrolle zeigt der Benutzer seine Cultur-Card und sein Ticket vor. Über einen Bar Code Leser werden die maschinenlesbaren Daten der CulturCard und des Tickets eingelesen und vom Rechner der Kontrollstation nach Kontrollverfahren A überprüft. Für die Überprüfung benötigt der Rechner den öffentlichen Part des Signaturschlüssels des Veranstalters. Alle anderen Daten stehen in maschinenlesbarer Form auf dem Ticket und der CulturCard.

Patentansprüche

1. Verfahren zur Bereitstellung von Berechtigungsnachweisen, insbesondere Eintrittskarten und Beförderungsscheinen, mit folgenden Schritten:

Erfassen von Ausgangsdaten über den Gegenstand der Berechtigung an einer ersten Datenverarbeitungsstation;

Zuweisen einer ersten Identifikationszeichen-

folge für den Berechtigungsnachweis;
- Bereitstellen eines Signaturschlüssels mit einem öffentlichen Teil und einem geheimen Teil;
- Erzeugen signierter Daten durch digitales Signieren zumindest der Ausgangsdaten und der ersten Identifikationszeichenfolge auf Basis des geheimen Teils des Signaturschlüssels;
- Übermitteln der signierten Daten über ein elektronisches Medium an eine zweite, von der ersten räumlich getrennte Datenverarbeitungsstation;
- Erstellen des Berechtigungsnachweises an der zweiten Datenverarbeitungsstation, indem die signierten Daten auf ein maschinenlesbares transportables Speichermedium übertragen werden, das als Berechtigungsnachweis dient.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß an der ersten Datenverarbeitungsstation weiterhin eine zweite Identifikationszeichenfolge für den öffentlichen Teil des Signaturschlüssels zugewiesen wird, wobei das Erzeugen signierter Daten durch digitales Signieren zumindest der Ausgangsdaten und der ersten und zweiten Identifikationszeichenfolge erfolgt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß an der ersten Datenverarbeitungsstation weiterhin eine dritte Identifikationszeichenfolge für ein Berechtigungsmedium oder ein aus dieser Identifikationszeichenfolge und einer Zufallszahl erzeugter Hashwert erfaßt wird, wobei die dritte Identifikationszeichenfolge oder der Hashwert ebenfalls digital signiert wird, und das Berechtigungsmedium mit der dritten Identifikationszeichenfolge unabhängig von der Bereitstellung des Berechtigungsnachweises bereitgestellt wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die dritte Identifikationszeichenfolge mittels der Technik der blinden Signatur oder der Hashwert digital signiert wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß vor dem Erfassen der Ausgangsdaten über den Gegenstand der Berechtigung die Ausgangsdaten oder Daten zur Bestimmung der Ausgangsdaten von der zweiten Datenverarbeitungsstation über das elektronische Medium an die erste Datenverarbeitungsstation übermittelt werden.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß das elektronische Medium ein Netzwerk, insbesondere das Internet ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß das Übermitteln der signierten Daten in Form einer Graphikdatei erfolgt.

8. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die signierten Daten in der zweiten Datenverarbeitungsstation in eine Graphikdatei umgewandelt werden.

9. Verfahren nach einem der Ansprüche 7 oder 8, dadurch gekennzeichnet, daß die Graphikdatei eine 2D Bar Code Repräsentation der signierten Daten und eine ASCII-Darstellung der Ausgangsdaten und der erfaßten oder zugewiesenen Identifikationszeichenfolgen enthält.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß das maschinenlesbare Speichermedium ein bedruckbarer Träger, insbesondere Papier ist, auf dem die signierten Daten in graphischer Darstellung ausgedruckt werden.

11. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß das maschinenlesbare Speichermedium ein auf einem Träger angeordneter Speicherchip ist.

12. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß das maschinenlesbare Speichermedium ein auf einem Träger angeordneter Magnetstreifen ist.

13. Berechtigungsnachweis, insbesondere Eintrittskarte oder Beförderungsschein, auf dem signierte Daten in maschinenlesbarer Form gespeichert sind, wobei die signierten Daten eine über einen Signaturschlüssel erzeugte digitale Signatur von Ausgangsdaten über den Gegenstand der Berechtigung und von einer ersten Identifikationszeichenfolge des Berechtigungsnachweises enthalten.

14. Berechtigungsnachweis nach Anspruch 13, dadurch gekennzeichnet, daß die signierten Daten weiterhin eine zweite Identifikationszeichenfolge für einen öffentlichen Teil des Signaturschlüssels enthalten.

15. Berechtigungsnachweis nach Anspruch 13 oder 14, dadurch gekennzeichnet, daß die signierten Daten weiterhin eine dritte Identifikationszeichenfolge für ein Berechtigungsmedium enthalten.

16. Berechtigungsnachweis nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, daß er aus einem bedruckbaren Träger, insbesondere Papier besteht, auf dem die signierten Daten in graphischer Darstellung, die eine maschinenlesbare Repräsentation beinhalten, aufgedruckt sind.

17. Berechtigungsnachweis nach Anspruch 16, dadurch gekennzeichnet, daß die signierten Daten in 2D Bar Code-Repräsentation und die Ausgangsdaten sowie die Identifikationszeichenfolgen in ASCII-Darstellung aufgedruckt sind.

18. Berechtigungsnachweis nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, daß er einen Speicherchip enthält, auf dem die signierten Daten gespeichert sind.

19. Berechtigungsnachweis nach einem der Ansprüche 13 bis 15, dadurch gekennzeichnet, daß er einen Magnetstreifen enthält, auf dem die signierten Daten gespeichert sind.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 198 23 907 A1
Int. Cl.[6]: G 07 F 7/08
Offenlegungstag: 2. Dezember 1999

Fig. 1

```
-----BEGIN SIGNED TICKET-----
CulturCard ID     74921068
Ticket ID         82349294
Key ID            F5CC06F1
Ort               English Theater
Veranstaltung     Much Ado about Nothing
Zeit              21.3.98, 19:30
Platz             Reihe 23, Platz 15
Kategorie         normal, 20,-
-----BEGIN SIGNATURE-----
iQCVAwUBNL3N5MXJpGaF/uwpAQEmcAQA1RZ8S+/gzYt4v9PgwZI9HQIX9ybgEY1h
HCxNkQPNJf9L9/jnqpUib7f0LNxmd5seirwTCpuloge34kR9Dgvp2K33W74rmR+G
BB4fvuaBmu6bOOiX6Ptc68i/DrSHHFrv4QF0pHzHOsJA2MxV9keFEk8+bDFNpppx
3YQVCEIBANQ=
=Lc0K
-----END SIGNATURE-----
```

Fig. 2

Nummer: DE 198 23 907 A1
Int. Cl.[6]: G 07 F 7/08
Offenlegungstag: 2. Dezember 1999

Fig. 3

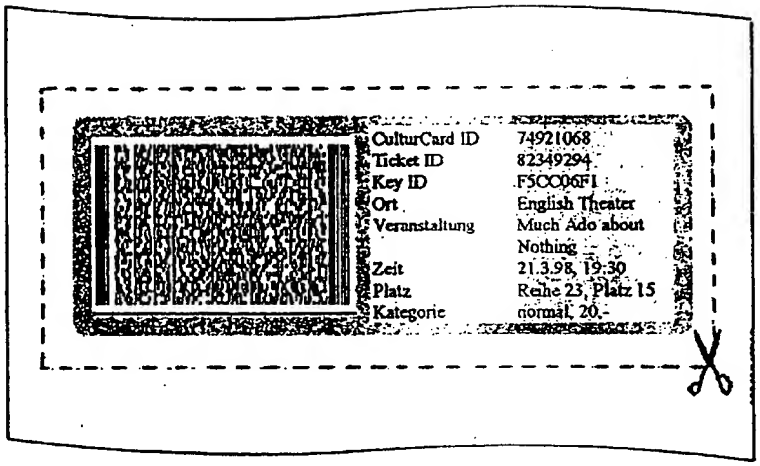

Fig. 4